BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) (11) Publication number: 11024916 A

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: 09181182

(22) Application date: 07.07.97

(51) Intl. Cl.: G06F 9/06 G06F 15/00 G09C 1/00 H04L 9/32

(30) Priority:

(43) Date of application publication: 29.01.99

(84) Designated contracting states:

(71) Applicant: FUJI XEROX CO LTD

(72) Inventor: KOJIMA SHUNICHI
NAKAGAKI JUHEI
KONO KENJI

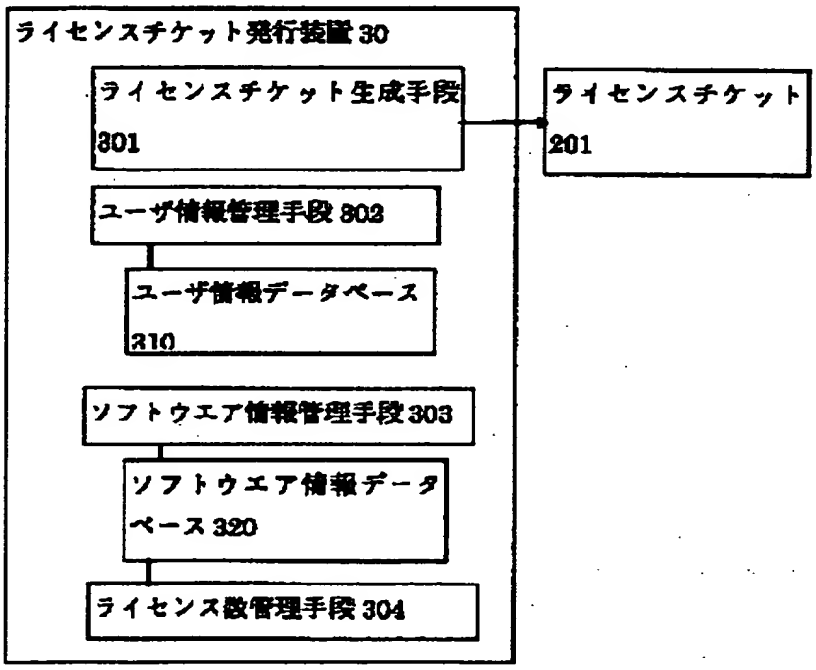
(74) Representative:

(54) DEVICE AND METHOD FOR MANAGING SOFTWARE LICENCE

(57) Abstract:

PROBLEM TO BE SOLVED: To control soft ware and to manage a license offline.

SOLUTION: User specific information dU is taken out form a user information data base 310 based on the request of a user and a secret key D is obtained from a software information data base 320. A license ticket (t) is generated by t=D-F(dU, n) and it is issued to the user. A function F is preferably a one- way hash function. The user can verify an access qualification to software by using the license ticket and user specific information to make use of the software. An item of the pertinent user of the user information data base 310 and an item of the pertinent user of the user information data base 320 are updated in accordance with issuance of the license ticket. Charging is executed based on the content of the software information data base 320 at an appropriate period.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－24916

(43)公開日　平成11年(1999)１月29日

(51)Int.Cl.⁶		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｃ
					５５０Ｇ
					５５０Ｚ
	15/00	３３０		15/00	３３０Ｅ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ

審査請求　未請求　請求項の数15　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平9－181182

(22)出願日　平成９年(1997)７月７日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　小島　俊一
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　河野　健二
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

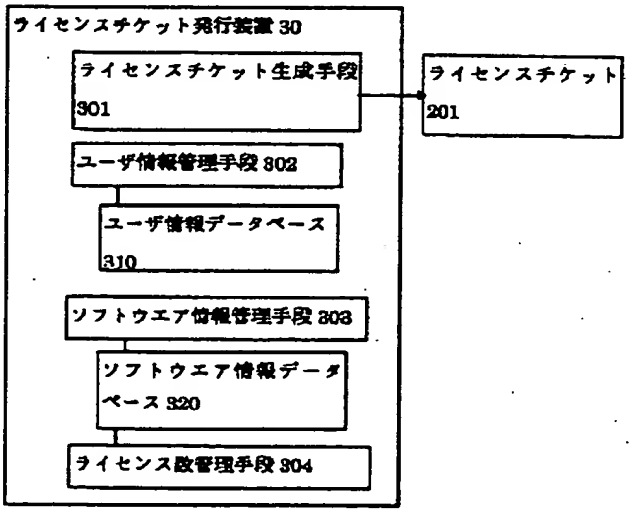
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　ソフトウェアライセンス管理装置および方法

(57)【要約】

【課題】　オフラインでもソフトウェアの実行制御を行えるようにし、あわせてライセンスの管理を行えるようにする。

【解決手段】　ユーザの要求に基づいて、ユーザ情報データベース３１０からユーザ固有情報ｄＵを取り出し、ソフトウエア情報データベース３２０から秘密鍵Ｄを得る。ライセンスチケットｔはｔ＝Ｄ－Ｆ（ｄＵ，ｎ）により生成され、ユーザに発行される。ユーザは、ライセンスチケットおよびユーザ固有情報を用いてソフトウェアのアクセス資格を証明でき、ソフトウェアを利用できる。ライセンスチケットの発行に応じて、ユーザ情報データベース３１０の該当ユーザの項目とソフトウエア情報データベース３２０の該当ソフトウエアの項目が共に更新される。適当な時期で、このソフトウエア情報データベース３２０の内容に基づき課金が行われる。



【特許請求の範囲】

【請求項１】　証明データ生成装置と、証明データ検証装置とを有し、
前記証明データ生成装置は、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、前記ユーザの固有情報とアクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを具備し、
上記証明データ検証装置は、
利用を制限されたソフトウェアを記憶するソフトウェア記憶手段と、
認証用データを記憶する第４の記憶手段と、
証明データを記憶する第５の記憶手段と、
前記第５の記憶手段に記憶されている前記証明データが、前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段と、
前記証明データ検証手段による検証が成功した時のみ、前記ソフトウェア記憶手段に記憶されている前記ソフトウェアの利用を可能にする実行制御手段とを具備し、
前記証明データ検証装置と、前記証明データ生成装置とが、互いに通信してユーザのアクセス資格認証をおこない、正当な前記証明用補助情報を有するユーザのみにソフトウェアの利用を可能にすることを特徴とするソフトウェアライセンス管理装置。

【請求項２】　前記ユーザ向けに前記証明用補助情報を発行する証明用補助情報発行装置をもち、発行の記録に基づいてソフトウエアの管理をおこなうことを特徴とする請求項１に記載のソフトウエアライセンス管理装置。

【請求項３】　前記ユーザ向けに前記証明用補助情報を発行する証明用補助情報発行装置を持ち、前記証明用補助情報を発行した数に基づいて、許諾したソフトウェアのライセンス数を管理することを特徴とする請求項１に記載のソフトウェアライセンス管理装置。

【請求項４】　前記証明用補助情報発行装置は、さらに前記証明用補助情報を発行可能な上限数を記憶する発行上限記憶手段と、既に発行し、かつ有効な証明用補助情報の数を記憶する第６の記憶手段と、前記第６の記憶手段に記憶されている有効ライセンス数が、前記発行上限記憶手段に記憶した上限数に達すると、それ以上の証明用補助情報の発行を行わないライセンス数管理手段をもつことを特徴とする請求項２または３に記載のソフトウェアライセンス管理装置。

【請求項５】　前記証明データ生成装置において、利用制御情報を記憶する利用制御情報記憶手段をさらに備え、前記証明データ生成手段は、前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報と、前記利用制御情報記憶手段に記憶されている前記利用制御情報とに所定の計算を施して証明データを生成し、前記ユーザの固有情報と、前記アクセス資格認証の特徴情報と、前記利用制御情報とに対し、所定の計算を実行した実行結果である証明用補助情報を有するユーザのみに前記ソフトウェアの利用を可能にすることを特徴とする請求項１、２、３または４に記載のソフトウェアライセンス管理装置。

【請求項６】　前記利用制御情報は、前記証明用補助情報の有効期間を示すデータを含むことを特徴とする請求項５に記載のソフトウェアライセンス管理装置。

【請求項７】　既に発行した前記利用制御情報の有効期間情報により、前記第６の記憶手段に記憶されている有効ライセンス数の更新をおこなうライセンス数管理手段をもつことを特徴とする請求項１、２、３、４、５または６に記載のソフトウェアライセンス管理装置。

【請求項８】　前記利用を制限されたソフトウエアは、少なくとも一部分を暗号化した状態で前記ソフトウエア記憶手段に記憶され、前記アクセス資格認証の特徴情報が暗号化関数における第１の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第２の復号鍵を前記第１の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ生成手段によって生成された証明データが前記第２の復号鍵であり、前記第２の復号鍵を用いて前記暗号化されたプログラムの一部分を復号して、前記プログラムの実行をおこなうことを特徴とする請求項１、２、３、４、５、６または７に記載のソフトウエアライセンス管理装置。

【請求項９】　少なくとも、前記第２の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項１、２、３、４、５、６、７または８に記載のソフトウエアライセンス管理装置。

【請求項１０】　少なくとも、前記第２の記憶手段と、前記証明データ生成手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項１、２、３、４、５、６、７または８に記載のソフトウエアライセンス管理装置。

【請求項１１】　前記利用を制限されたソフトウエアをもつ前記証明データ検証装置をＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどの媒体に格納して流通可能にしたことを特徴とする請求項１から１０に記載のソフトウエアライセンス管理装置。

【請求項１２】　前記利用を制限されたソフトウエアをもつ前記証明データ検証装置をＷＷＷサーバやＦＴＰサ

ーバなど、ネットワーク上のサーバのサービスとして流通可能にしたことを特徴とする請求項１、２、３、４、５、６、７、８、９または１０に記載のソフトウエアライセンス管理装置。

【請求項１３】　少なくともユーザの固有情報とソフトウェアのアクセス資格認証の特徴情報とに基づいて認証用補助情報を発行する手段と、

前記証明用補助情報を発行した数に基づいて、許諾したソフトウェアのライセンス数を管理する手段とを有することを特徴とするソフトウェアライセンス管理用の認証用補助情報発行装置。

【請求項１４】　前記証明用補助情報の発行可能な上限数を記憶する発行上限記憶手段と、

既に発行し、かつ有効な証明用補助情報の数を記憶する有効ライセンス数記憶手段とをさらに有し、

前記ライセンス記憶手段に記憶されている有効ライセンス数が、前記発行上限記憶手段に記憶した上限数に達すると、それ以上の証明用補助情報の発行を行わないようにすることを特徴とする請求項１３に記載のソフトウェアライセンス管理用の認証用補助情報発行装置。

【請求項１５】　認証用データを記憶する第１の記憶ステップと、

ユーザの固有情報を記憶する第２の記憶ステップと、前記ユーザの固有情報とアクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶ステップと、

前記第１の記憶ステップによって保持されている認証用データと、前記第２の記憶ステップによって記憶されている前記ユーザの固有情報と、前記第３の記憶ステップによって記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成するステップと、

利用を制限されたソフトウェアを記憶するステップと、

認証用データを記憶する第４の記憶ステップと、

証明データを記憶する第５の記憶ステップと、

前記第５の記憶ステップによって記憶されている前記証明データが、前記アクセス資格認証の特徴情報に基づいて生成されていることを検証するステップと、

前記検証が成功した時のみ、前記ソフトウェアの利用を可能にするステップとを有することを特徴とするソフトウェアライセンス管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ソフトウエアのライセンスを管理する方法とその装置に関する。

【０００２】

【従来の技術】従来、ソフトウエアは、フロッピーディスク等の物理媒体に格納され、物理媒体として売買されてきた。しかし、ソフトウエアのようなディジタル著作物は、オリジナルと寸分違わぬコピーを容易に作成することが可能であるという特質を持つために、簡単に不正コピーされて使われることが多かった。近年、磁気ディスクなどコンピュータの記憶容量が大容量化されるにつれて、この不正コピーの数は増大しているといわれている。

【０００３】ソフトウエアは、ソフトウエアのプロバイダーとユーザとの間で、ライセンス契約（使用許諾契約）を結んで使用することが多いが、上述したようにソフトウエアは容易にコピーが可能であるため、ライセンス契約を行わずに不正コピーしたソフトウエアを利用するユーザも多い。

【０００４】また、企業や大学においても、社員や学生が企業内や大学内のコンピュータに勝手にソフトウエアを不正コピーして使用しているかどうかを把握する術がないため、知らぬ間に大量の不正コピーが行われていて、時に摘発されて、信用の失墜と膨大な賠償を被ることにもなりかねない。

【０００５】このような状況に対して、近年ライセンス管理システムと呼ばれるものが開発されてきている。ライセンス管理システムは、ライセンスを許可されていないユーザには、ソフトウエアの利用ができないように構成されたものであり、ソフトウエアを暗号化して配布したり、パスワードによる実行制御によって、利用制限をおこなっている。

【０００６】しかし、パスワードを他人に教えたり、暗号鍵ごとコピーして使ったりすることにより、結局は不正コピーと変わらない状況になってしまう。

【０００７】そこで、一つの解決方法として、米国Ｓａｓｓａｆｒａｓ社のＫｅｙＳｅｒｖｅｒ（商標）に代表されるような、ネットワーク上のライセンス管理サーバによって実行可能数を管理する方法が考えられている。この管理手法では、オリジナルのソフトウエアを暗号化などの方法で利用を制限し、それを公開する。オリジナルのソフトウエアは別に管理者しかアクセスできないところに物理的に鍵を掛けて保存する。ユーザはソフトウエア実行時にライセンスサーバからライセンス（鍵）の供与を受け、実行制御を解除し利用している。オンラインで発行されたライセンス（鍵）がなければソフトウエアは実行することができず、発行された鍵はユーザには見えないようにすることで不正使用を防止している。

【０００８】

【発明が解決しようとする課題】しかし、このようなネットワーク上のライセンスサーバによる管理方式では、オフライン時での使用制限をおこなうことが不可能である。ネットワークにアクセスし難いモバイル環境でも、正当なライセンスをもつ場合は正当にソフトウエアを実行出来ることが必要である。つまり、ユーザにオンライン・オフライン両方の環境下で、同じように実行制御が可能で、かつ不正な二次コピーの配布を防止出来る仕組みにすることが必要である。本発明は、上記従来の課題を解決し、オフラインでも実行制御ができるソフトウェ

アライセンス管理装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明によれば、上記目的を達成するに、所定の手法たとえば暗号化によってその利用を制限したソフトウエアに対して、ユーザのアクセス資格を認証する証明データ検証手段を設ける。他方、ユーザ側には、そのソフトウエアを利用できることを示す証明データ生成手段を設け、証明データ検証手段と証明データ生成手段とが相互に通信してユーザのアクセス資格を検証する。さらに、ソフトウエア側に、以上の検証結果が成功したときのみソフトウエアの復号等を行いプログラムを実行できるようにする実行制御手段を設ける。また、証明データを生成する際にはユーザの固有情報と証明用補助情報とが必要であり、所定の発行装置が、ユーザの固有情報とソフトウエアのライセンス情報に基づいて証明用補助情報を発行する。

【００１０】この構成においては、ユーザはユーザの固有情報に対応する真正な証明補助情報を有していなければプログラムを実行させることができない。そしてこの証明補助情報を発行する装置が、証明補助情報の発行管理を通じてソフトウェアライセンスを管理することができる。

【００１１】

【発明の実施の態様】以下、本発明の実施例について説明する。

［全体の構成］図１は、本発明の一実施例の構成を全体として示している。図１において、証明データ検証装置１０はソフトウェアプロバイダにより提供される。この証明データ検証装置１０は、利用を制限されたソフトウエア１００を含み、さらに証明データ検証手段１１０と実行制御手段１２０とを有している。証明データ検証手段１１０は認証用データ１１１を生成し、証明データ生成装置２０が管理する証明データ生成手段２００に送る。ここでの通信手段は特に問わない、プロセス間の通信であってもネットワークを介した通信でも構わない。証明データ生成手段２００は受け取った認証用データ１１１とその証明データを生成するのに必要なライセンスチケット２０１とユーザ固有情報２０２とから証明データ２０３を生成し、証明データ検証手段１１０に送る。証明データ検証手段１１０は、証明データ生成手段２００から生成された証明データ２０３を受け取り、検証をおこなう。検証結果によって、実行制御手段１２０で利用制限を解除しソフトウエア１００を利用できるようにする。

【００１２】ユーザは証明データ生成に先立ち、ライセンスチケット２０１をライセンスチケット発行装置３０から発行してもらう。ライセンスチケット発行装置３０はライセンスチケットをユーザの固有情報２０２とアクセス資格認証の特徴情報３００とから生成する。

【００１３】なお、この実施例においては、図２に示すように、有効期限等の利用制限情報２０４を用いて利用を制限するようにしてもよい。図２において、図１と対応する箇所には対応する符号を付して詳細な説明を省略する。また、図１および図２において、証明データ生成装置２０中において点線で囲んだ部分は耐タンパー装置で防御されている部分を部分を示す。

【００１４】［アクセス資格認証の概略］以下に本実施例を詳細に説明する。まず、アクセス資格の認証について説明する。ユーザのアクセス資格の認証には、暗号化の手法が使用されるが、この例においてはＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｅｌｍａｎ）公開鍵暗号系を用いる。もちろん、他の種々の暗号を用いることができる。

【００１５】まず、ソフトウエアに対して認証用の公開暗号鍵ペアとして公開鍵Ｅと秘密鍵Ｄとそれに対する法数ｎとを設定する。法数ｎはソフトウエアに対して設定する。ライセンス資格認証の特徴情報３００としてこの秘密鍵Ｄを使用する。

【００１６】この実施例では、以下の情報または計算を用いてライセンス資格の認証を行う。

①共通鍵暗号の鍵Ｋ：プログラムの少なくとも一部を暗号化して利用制限する。

②ユーザ固有情報ｄＵ

③ライセンス資格認証の特徴情報Ｄ

④ライセンスチケットｔ＝Ｄ－Ｆ（ｄＵ，ｎ）またはＤ－Ｆ（ｄＵ，ｎ，Ｌ）

ただし、Ｆ（）は好ましくは一方向ハッシュ関数である。Ｌは有効期限等の利用制限情報である。

⑤認証用データ$C = r^{E}K^{E} \pmod{n}$

ただし、ｒは乱数である。

⑥証明データ生成式：$C^{t}C^{F(dU,n)}$または$C^{t}C^{F(dU,n,L)} \pmod{n}$

⑦検証手法：乱数効果を除去して鍵Ｋを復元し、暗号化プログラムを復号する。

【００１７】証明データ検証装置１０と証明データ生成装置１１とは相互にデータを通信して認証を行い、認証が成功するとソフトウェアを利用することが可能となる。認証は、まず、ソフトウェア利用の要求に応じて、証明データ検証装置１０が認証用データ（ＣまたはＣ＝$r^{E}K^{E}$）１１１を証明データ生成装置１１に送出し、証明データ生成装置１１は、この認証用データ１１１とユーザ固有情報（ｄＵ）２０２とライセンスチケット（ｔ＝Ｄ－Ｆ（ｄＵ，ｎ））２０１と対して所定の演算を実行して証明データ２０３を生成し、証明データ検証装置１０に返す。ライセンスチケット（ｔ）と、ユーザ固有情報（ｄＵ）と、認証の特徴情報（Ｄ，ｎ）が対応していれば、証明データは、$(rK)^{ED} \bmod n$となり、$DE \bmod n = 1$から、ｒＫとなる。そして、乱数ｒを用いてＫを算出する。この共通暗号鍵Ｋを用いて暗号化されているソフトウェアを復号して実行する。

【００１８】［ソフトウェアの利用制限手法］つぎに、ソフトウェアの利用制限について説明する。この実施例では、ソフトウェアの利用制限の手法としては、共通鍵暗号系による暗号化を採用する。利用制限されたソフトウェア１００（図１、図２）は図３に示すように予め処理されて、頒布される。図３において、まず、ソフトウェアの少なくとも一部を共通鍵暗号の鍵Ｋで暗号化する（Ｓ１０）。つぎに鍵ＫをＲＳＡ暗号の公開鍵Ｅで暗号化し（Ｓ１１、$K'=K^E \mod n$）、暗号化した鍵Ｋ’を証明データ検証手段１１０が取り出せる状態でソフトウェアに埋め込む（Ｓ１２）。

【００１９】［認証用データ］つぎに認証用データ１１１の一例を説明する。認証用データ１１１は、この例では、$C=r^EK' \mod n$である。ただし、ｒは乱数である。認証用データは、図４に示すように生成される。まず、暗号化された秘密鍵データＫ’を取り出す（Ｓ２１）。つぎに乱数ｒを設定し、乱数ｒは保持しておく（Ｓ２２）。そして$C=r^EK' \mod n$を計算し、Ｃの値とｎとの組みを認証用データ１１１とする。ここで、乱数ｒは毎回変化し予測不可能なので、同じ証明データを再度使用できないようにする。したがってリプレイアタックに対処できる。

【００２０】［ライセンス管理手法ーライセンスチケット発行］つぎに、ソフトウエアのライセンス管理の例を説明する。この例においては、ユーザが使用するソフトウエアに対するライセンスチケットの発行枚数に応じて、各ソフトウエアのプロバイダにライセンスフィーを支払うようになっている。

【００２１】図５は、この管理例で用いるライセンスチケット発行装置３０の構成をしめす。このライセンスチケット発行装置３０は、ユーザの要求により、ユーザの証明データ生成に必要なライセンスチケット（ｔ）２０１を生成し発行する装置である。

【００２２】図５において、ライセンスチケット発行装置３０は、ライセンスチケット生成手段３０１、ユーザ情報管理手段３０２、ユーザ情報データベース３１０、ソフトウェア情報管理手段３０３、ソフトウェア情報データベース３２０およびライセンス数管理手段３０４を含んで構成されている。

【００２３】なお、先に説明したユーザ固有情報２０２とライセンス資格認証の特徴情報３００としてのソフトウエアの秘密鍵Ｄとは、安全に秘密情報として管理されていなくてはならない。ユーザ固有情報（ｄＵ）２０２はユーザＵに対する秘密情報でユーザ情報データベース３１０に安全に保存されている。ユーザへは証明データ生成手段２００（図１）の一部として、安全な保護容器（例えばＩＣカード）の中に保持されて渡される。この手順に関係する構成は本発明では限定しない。たとえば、別の第三者がこの配布をおこなってもよいし、ライセンスチケット発行装置３０がこの機能を兼ねていてもかまわない。ユーザデータベース３１０へのアクセスはユーザ情報管理手段３０２によっておこなわれる。

【００２４】図６はユーザ情報データベース３１０の構成例を示す。図６に示すように、ユーザ情報データベース３１０では、ユーザの識別子としてユーザＩＤをもち、ユーザ名Ｕ、ユーザ固有情報ｄＵ、発行したライセンスチケットの履歴をリスト形式で持っている。ユーザ情報データベース３１０を参照することにより、ユーザごとの発行したライセンス枚数や発行の履歴を調べることができる。

【００２５】ソフトウエアに関する秘密鍵Ｄ（資格認証の特徴情報３００）はライセンスチケット発行装置３０が生成して、公開鍵Ｅをソフトウエアプロバイダに配布するか、または逆にソフトウエアプロバイダから秘密鍵Ｄを安全な手段で受け取り管理する方法が考えられる。このソフトウエアに対する公開鍵秘密鍵のペアの生成に関する構成は本発明では限定しない。秘密鍵Ｄはソフトウエア情報データベース３２０で安全に保持され、ソフトウエア情報管理手段３０３によって管理される。

【００２６】図７は、ソフトウエア情報データベース３２０の構成例を示す。図７に示すように、ソフトウェア情報データベース３２０では、ソフトウエアのＩＤや名称、ＲＳＡ法数ｎ、秘密情報Ｄの他に、ライセンスチケットの発行枚数、必要ならばそのリストを保持することにする。ソフトウエア情報データベース３２０によって、そのソフトウエアに対して何枚のライセンスチケットが発行されているかを確認できることとなる。

【００２７】図８は、ライセンスチケットの生成方法とそれに伴うデータベース３１０、３２０への操作を示す。図８において、まず、ユーザの要求により、発行するライセンスチケットのユーザＵとソフトウエアｎの情報を得る。すなわち、ユーザ情報データベース３１０からユーザ固有情報ｄＵを取り出し（Ｓ３０）、ソフトウエア情報データベース３２０から秘密鍵Ｄを得る（Ｓ３１）。ライセンスチケットｔはつぎの生成式により生成される（Ｓ３２）。

【００２８】

【数１】$t=D-F(dU, n)$

ここでの関数Ｆ（）は、上述のとおり、好ましくは一方向性ハッシュ関数である。関数の引数の各項は、単純な接合が考えられる。が本発明ではこれに限らない。すべての項目が関数の結果に影響するようなものであればどのような方式でもかまわない。

【００２９】最後にユーザ情報データベース３１０の該当ユーザの項目とソフトウエア情報データベース３２０の該当ソフトウエアの項目を共に更新する（Ｓ３３）。

【００３０】適当な時期で、このソフトウエア情報データベース３２０の内容を調べて、各ソフトウエアに対するライセンスチケットの発行枚数によりソフトウエアプロバイダへライセンスフィーを支払う。

【００３１】［他のライセンス管理手法］つぎに、ソフトウエアのライセンス管理の別の例を説明する。このライセンス管理の方法は、予め各ソフトウエアにはライセンス数の上限が設定されており、ライセンスチケットの枚数がその上限を超えては発行できないようにするものである。さらに、ライセンスチケットには有効期限を設ける。これにより、ライセンスチケットの失効の時間がくればソフトウエアは利用できなくなるので、新たな発行が可能になる。

【００３２】図９は、この管理手法に用いるソフトウエア情報データベース３２０の構成例を示す。図９に示すように、このソフトウェア情報データベース３２０では、ソフトウエアのＩＤや名称、ソフトウエアにユニークなＲＳＡ法数ｎ、秘密情報Ｄの他に、予め設定されたライセンス数、現在の有効ライセンスチケット数と、必要ならばそのリストを保持することにする。このソフトウエア情報データベース３２０によって、そのソフトウエアに対して同時に設定されたライセンス数（上限）までのライセンスチケットが発行することができる。

【００３３】図１０は、この管理手法にしたがうライセンスチケットの生成方法とそれに伴うデータベース３１０、３２０への操作を示す。図１０において、まず、ユーザの要求により、発行するライセンスチケットのユーザＵとソフトウエアｎの情報を得る。すなわち、ユーザ情報データベース３１０からユーザ固有情報ｄＵを取り出し（Ｓ４０）、ソフトウエア情報データベース３２０から現在のライセンスチケット数が設定された上限を超えないかを調べて、現在のライセンスチケットの発行の可否を決める（Ｓ４１、Ｓ４２、Ｓ４３）。発行が可能ならば、ソフトウエア情報データベース３２０から秘密鍵Ｄを取り出す（Ｓ４６）。発行が不可能であれば、その旨をユーザに通知する（Ｓ４５）。

【００３４】ライセンスチケットには利用制限情報Ｌを付属させることができる（Ｓ４７）。これにより、例えば、ライセンスに有効期間を設定し、この結果、有効期間を過ぎた場合（または、有効期間前）使用することができないライセンスチケットを作成することができる。この場合、ライセンスチケットｔはつぎの生成式で生成されて発行される（Ｓ４８）。

【００３５】

【数２】ｔ＝Ｄ－Ｆ（ｄＵ，ｎ，Ｌ）

ここでの関数Ｆ（）は、上述のとおり、好ましくは一方向性ハッシュ関数である。関数の引数の各項は、単純な接合が考えられるが、本発明ではこれに限らない。すべての項目が関数の結果に影響するようなものであればどのような方式でもかまわない。

【００３６】最後にユーザ情報データベース３１０の該当ユーザの項目とソフトウエア情報データベース３２０の該当ソフトウエアの項目を共に更新する（Ｓ４９）。

【００３７】このライセンス管理方式では、予め設定したライセンス数を超えてのユーザへの使用は不可能なので、ソフトウエアプロバイダへはその数のライセンスフィーを支払う。

【００３８】［証明データ生成］図１１は、証明データ２０３の生成方法の一例を示す。ここでは図９を参照して説明した管理手法に即して説明する。図１１において、まず、証明データ検証装置１０から認証用データ（Ｃ，ｎ）を受け取る（Ｓ５０）。つぎに受け取った認証用データ（Ｃ，ｎ）のｎの値に基づいて、ソフトウェア情報データベース３２０を参照して、対応するライセンスチケット（ｔ）２０１と利用制限情報Ｌを取得する（Ｓ５１）。このライセンスチケット２０１は、前述の方法でライセンスチケット発行装置３０より発行される。次に、ライセンスチケットの利用制限情報をチェックする（Ｓ５２）。例えば利用制限情報が有効期間であれば、現在時刻と比較する。利用が許容される場合には、つぎの式にしたがって証明データＲを生成する（Ｓ５３）。

【００３９】

【数３】$R = C^{t} C^{F(dU,n,L)}$

利用制限情報ＬとｔＤ－Ｆ（ｄＵ，ｎ，Ｌ）とは組で構成され、Ｌの中に有効期間などの制限情報を織り込まれている。ユーザはＬの偽造をおこなっても、対応するライセンスチケットｔの偽造は不可能なので、ライセンスチケットの完全性は保たれている。

【００４０】また、証明データの計算に必要なユーザ固有情報ｄＵは安全に保持・実行されなければならないので、ユーザ固有情報を保持する部分、および証明データの計算を計算する部分を、一般にはＩＣカードのような外部からの観測を困難にするような小型演算装置を持ったデバイスで実装することが要望される。

【００４１】［証明データ検証］図１２は、証明データ２０３の検証と、そこから得られたＫによる実行制御手段１２０によるソフトウエアの復号化の一例を示す。図１２において、まず、証明データ検証装置１０は証明データ生成装置２０から証明データＲを受け取る（Ｓ６０）。証明データ検証手段１１０は、受け取った証明データＲ２０３をソフトウエアの公開鍵Ｅで暗号化（署名検証）をして、ｒＫを得る（Ｓ６１）。この乱数ｒの項を除去することが出来るのは、証明データ検証装置１０のみである。ｒの項を除去し、Ｋを得る（Ｓ６２）。実行制御手段１２０は、この得られたＫの値をもって、利用を制限されたソフトウエア１００を復号化して、実行をおこなう（Ｓ６３）。

【００４２】以上説明したように、利用制限をされたソフトウエアに対する証明用補助情報としてのライセンスチケットをつかって、ユーザのアクセス資格を検証することにより、ソフトウエアの実行を可能にすることができる。ライセンスチケットの発行を管理することにより、ソフトウエアプロバイダへの正しい利用料（ライセ

ンスフィー）を支払うことが可能になる。また第二の実施例で説明したように、ライセンスチケットの発行を予め定められたライセンス数の上限まで発行する管理をすることも可能になる。もちろん、これらの認証動作は全でローカルな環境で実行されるので、ソフトウエア利用時にオンラインである必要が全くない。

【００４３】本発明によるソフトウエアは利用制限がかかっており、それ単体では動作は不可能なので、ＣＤ－ＲＯＭにいれて配布したり、インターネット上のＷＷＷサーバやＦＴＰサーバなどに置くことが可能である。利用したいユーザはライセンスチケットを購入してソフトウエアの利用制限を解除して使用することができる。ライセンスチケットの有効期間を短くすることにより、一ライセンスチケットの発行に対しての代金を安く設定して、安く多量に販売するというライセンス形態も可能になる。

【００４４】なお、本発明は上述の実施例に限定されるものではなく、種々変更が可能である。例えば、アクセス資格認証にＲＳＡ公開鍵暗号系の手法を使用したが、他の暗号系も適用可能である。

【００４５】

【発明の効果】以上説明したように、本発明によれば、ソフトウエアの二次使用による不正使用をオンラインでも、オフラインでも防止することが可能になり、正当なライセンス管理システムを構築できる。

【図面の簡単な説明】

【図１】　本発明の実施例のライセンス管理装置の概略を示すブロック図である。

【図２】　上述実施例の変形例を示すブロック図である。

【図３】　上述実施例のソフトウエアの暗号化の一例を示す図である。

【図４】　上述実施例の認証用データの生成方法の一例を示す図である。

【図５】　上述実施例のライセンスチケット発行装置の一例を示す図である。

【図６】　上述実施例のユーザ情報データベースの一例を示す図である。

【図７】　上述実施例のソフトウエア情報データベースの一例を示す図である。

【図８】　上述実施例のライセンスチケットの生成方法の一例を示す図である。

【図９】　上述実施例のソフトウエア情報データベースの別の例を示す図である。

【図１０】　上述実施例のライセンスチケットの生成方法の別の例を示す図である。

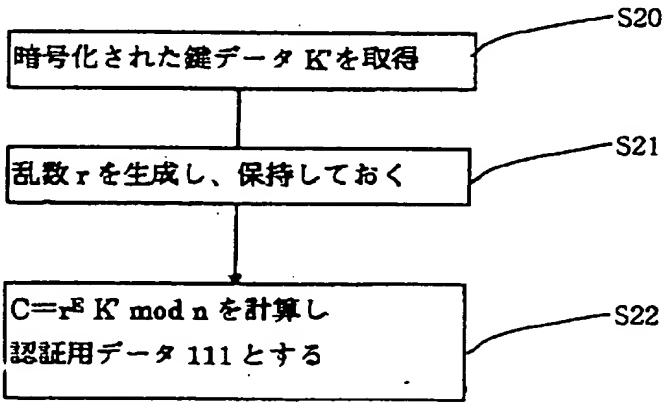
【図１１】　上述実施例の証明データ生成方法の一例を示す図である。

【図１２】　上述実施例の証明データ認証手段と実行制御手段の動作を示す図である。

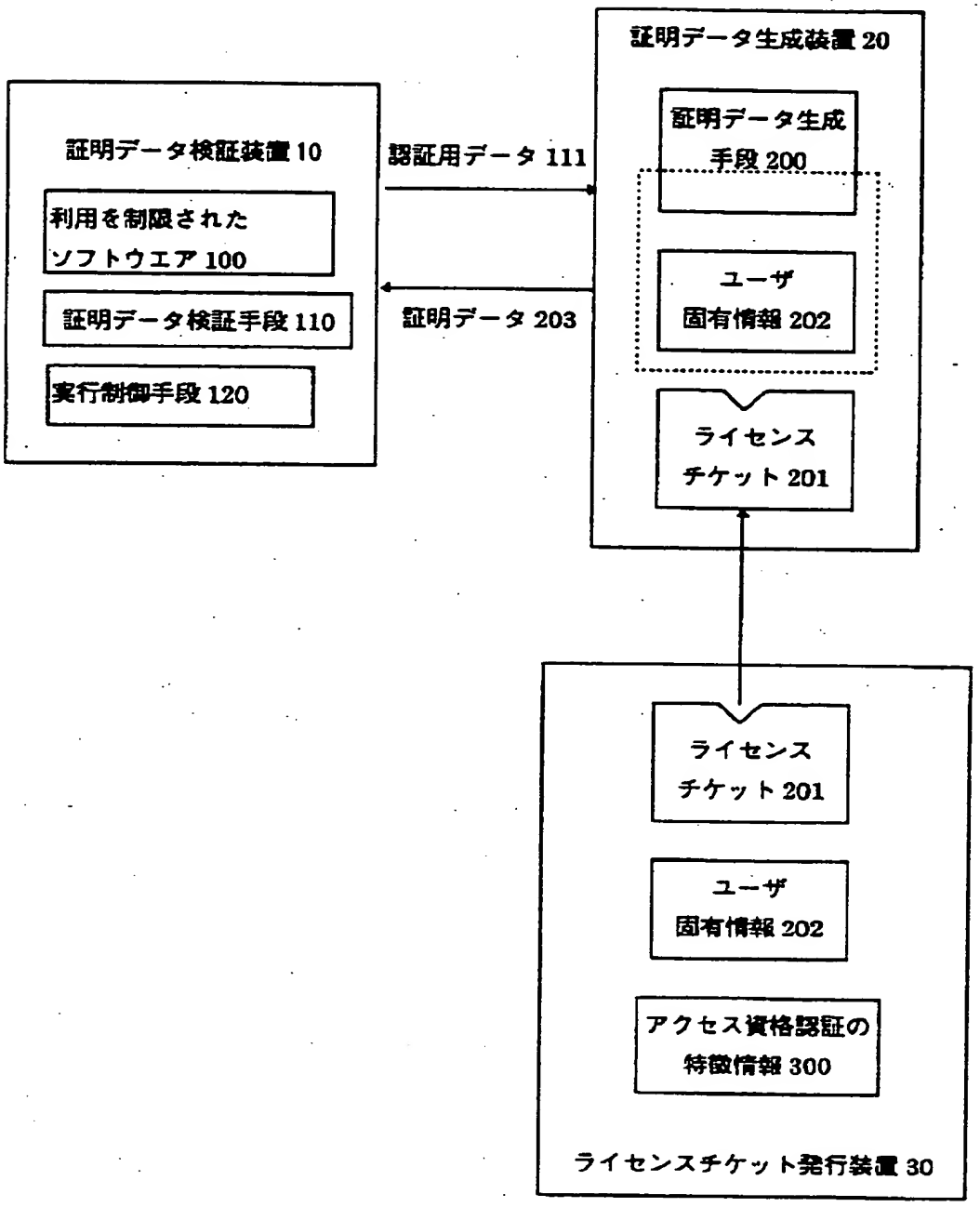
【符号の説明】

１０　証明データ検証装置
２０　証明データ生成装置
３０　アクセスチケット生成装置
１００　利用を制限されたソフトウェア
１１０　証明データ検証手段
１２０　実行制御手段
２００　証明データ生成生手段
２０１　ライセンスチケット
２０２　ユーザ固有情報
３００　アクセス資格認証の特徴情報
３０１　ライセンスチケット生成手段
３０２　ユーザ情報管理手段
３０３　ソフトウェア情報管理手段
３０４　ライセンス数管理手段
３１０　ユーザ情報データベース
３２０　ソフトウェア情報データベース

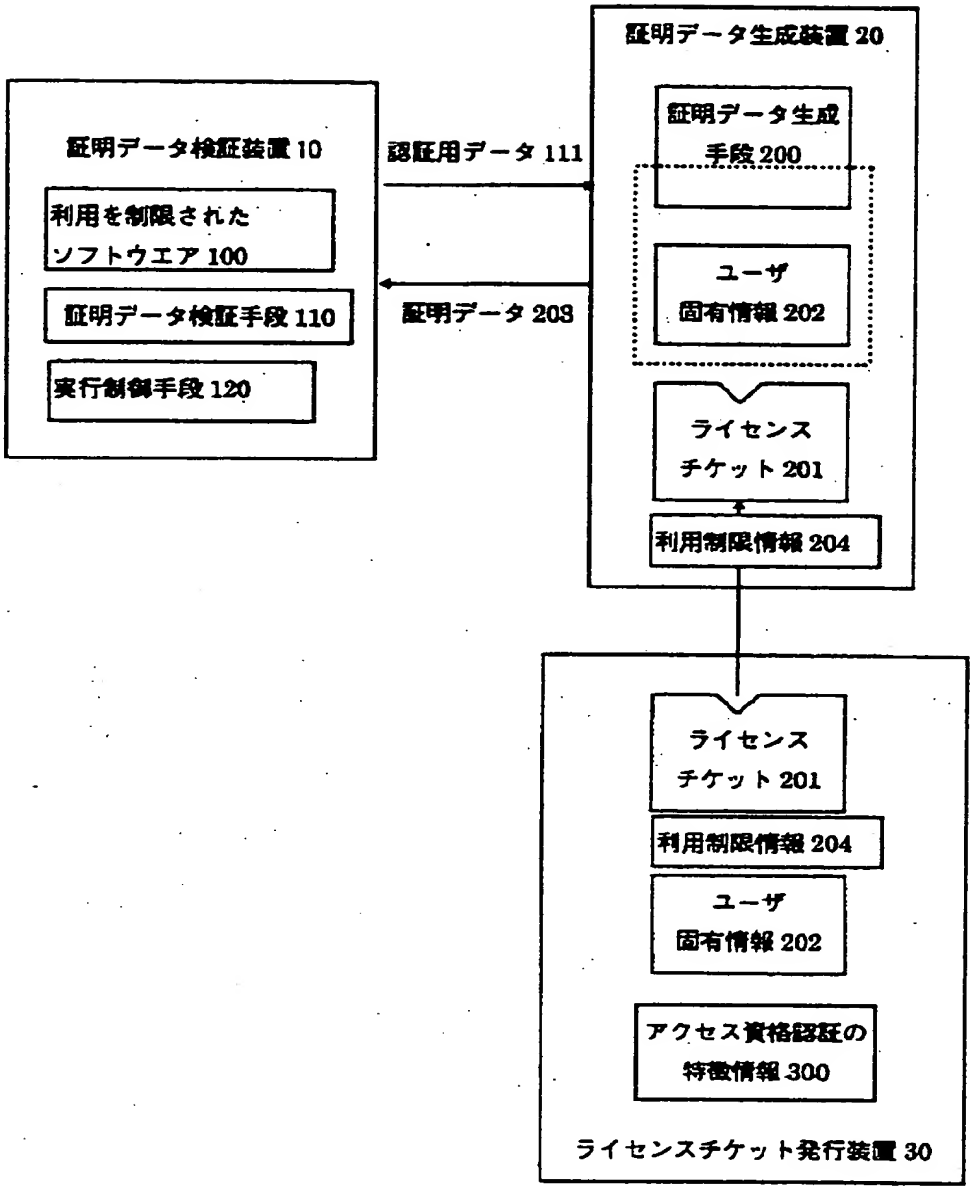
【図４】



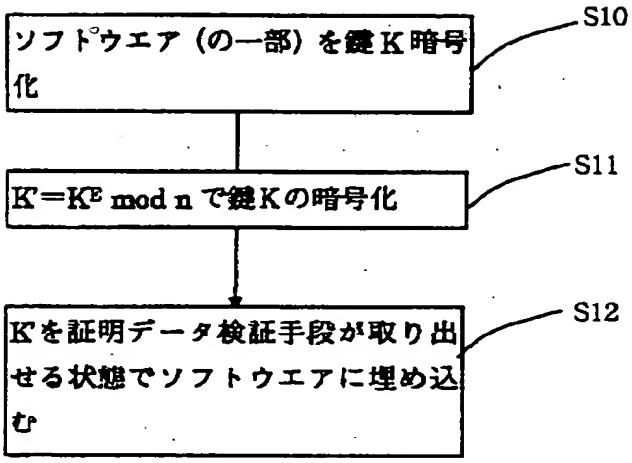
【図１】


証明データ生成装置 20
証明データ生成手段 200
ユーザ固有情報 202
ライセンスチケット 201
証明データ検証装置 10
利用を制限されたソフトウエア 100
証明データ検証手段 110
実行制御手段 120
認証用データ 111
証明データ 203
ライセンスチケット 201
ユーザ固有情報 202
アクセス資格認証の特徴情報 300
ライセンスチケット発行装置 30

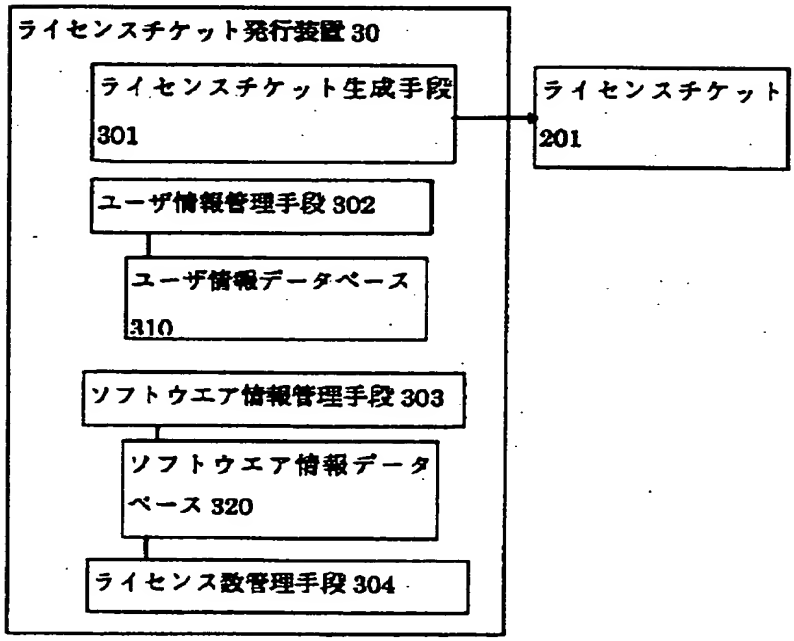
【図２】


証明データ生成装置 20
証明データ生成手段 200
ユーザ固有情報 202
ライセンスチケット 201
利用制限情報 204
証明データ検証装置 10
利用を制限されたソフトウエア 100
証明データ検証手段 110
実行制御手段 120
認証用データ 111
証明データ 203
ライセンスチケット 201
利用制限情報 204
ユーザ固有情報 202
アクセス資格認証の特徴情報 300
ライセンスチケット発行装置 30

【図３】



【図５】



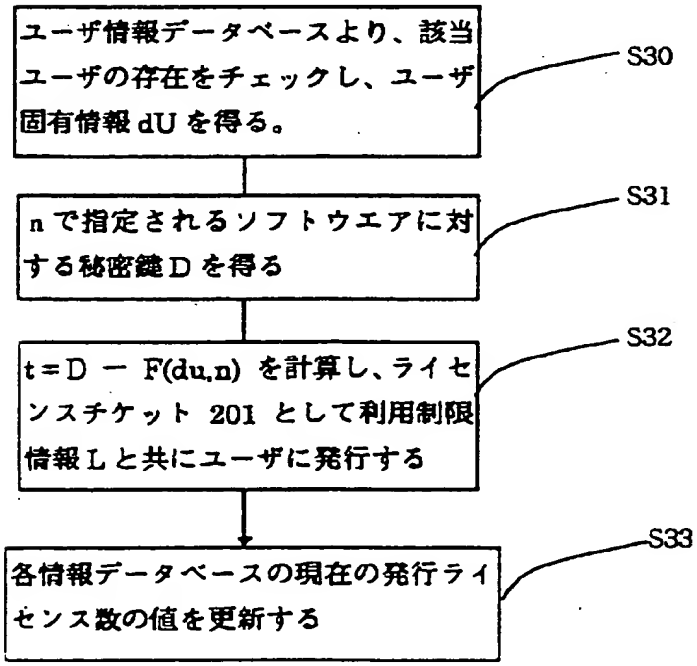
【図６】

ユーザID	ユーザ名U	ユーザ固有情報dU	チケット数	ライセンスチケットリスト
16047	s.kojima	1239042....	4	
17440	j.nakagaki	6756923...	7	

【図７】

Software ID	Software名	公開情報 (n)	秘密情報 (D)	発行チケット数	ライセンスチケットリスト
10001	Gloval View	3849214...	34355.....	33	
10002	Docu Works	6432876...	61321....	19	

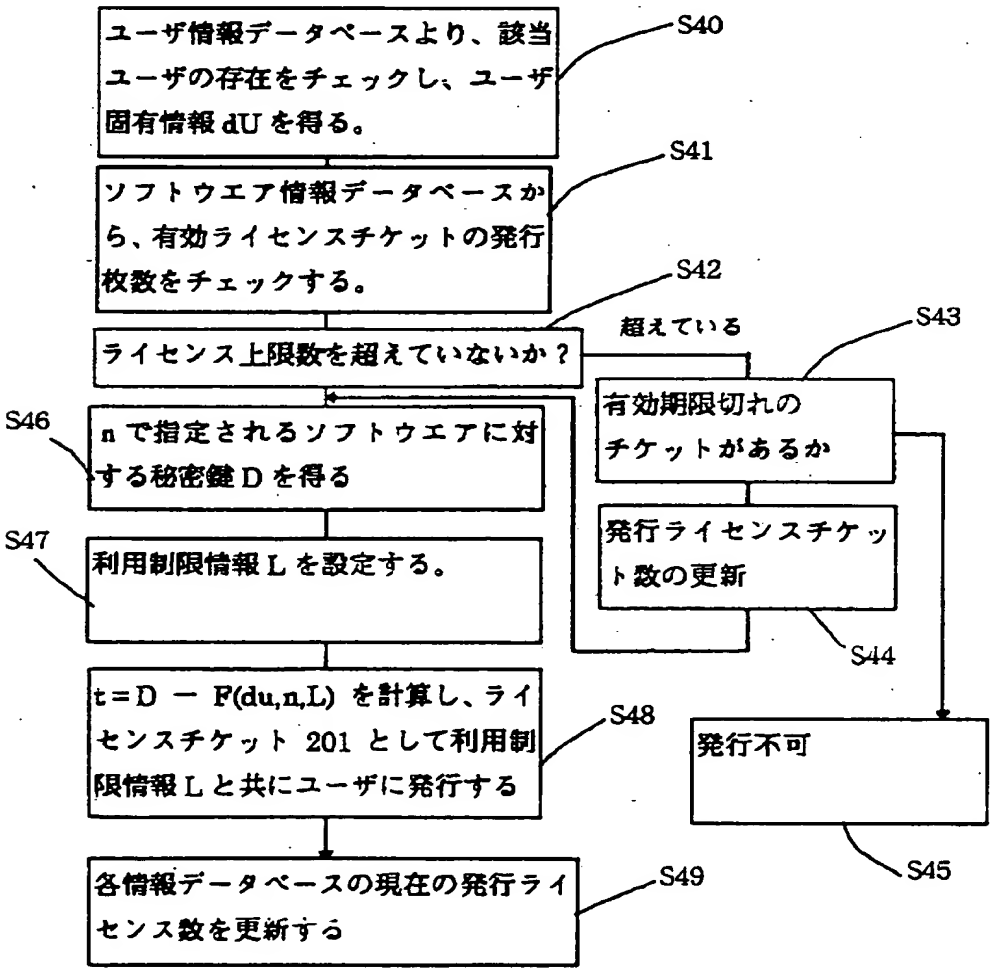
【図８】



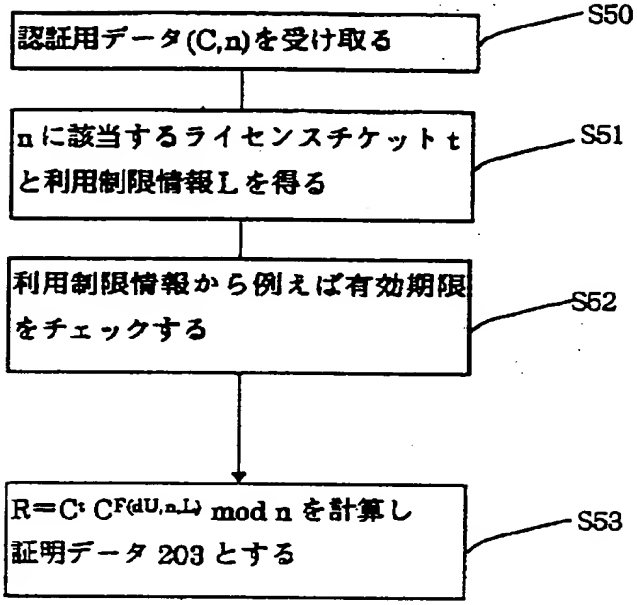
【図9】

Softw are ID	Software名	公開情報 (n)	秘密情報 (D)	設定ライセンス数	有効チケット数	ライセンスチケットリスト
10001	Gloval View	3849214..	34355.....	50	39	
10002	Docu Works	6432876..	61321....	20	19	

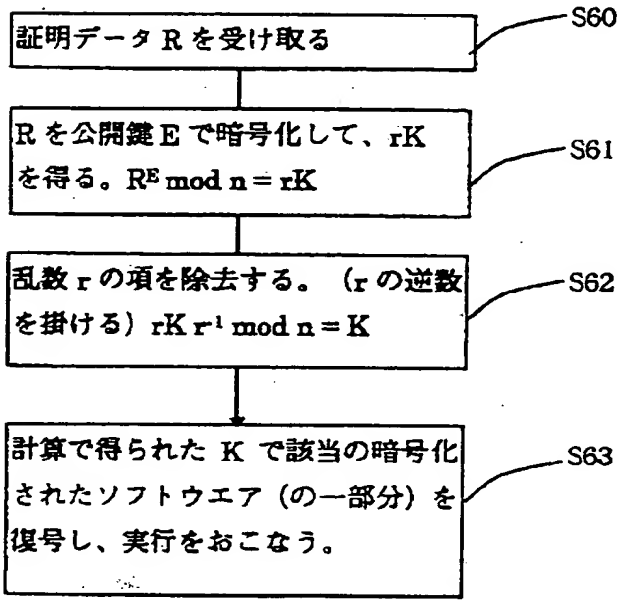
【図10】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
G09C	1/00	640	G09C	1/00	640E
H04L	9/32		H04L	9/00	675B